# IS-18 Data Retention Policy

**14.1 Data Retention Policy**

This policy specifies how important documents (hard copy, electronic or other media) should be retained, protected and destroyed. The policy also ensures that documents are promptly provided to authorities in the course of legal investigations or lawsuits.

**Document Retention Schedule**

The following types of documents will be retained for the following periods of time. At least one copy of each document will be retained according to the following schedule.

**Corporate Records**

|  |  |
| --- | --- |
| Article of Incorporation to apply for corporate status | Permanent |
| Bylaws | Permanent |
| Board policies | Permanent |
| Resolutions | Permanent |
| Board Meeting Minutes | Permanent |
| Sales Tax Exemption Documents | Permanent |
| Tax or employee identification number designation | Permanent |
| Annual corporate filings | Permanent |

**Financial Records**

|  |  |
| --- | --- |
| Chart of Accounts | Permanent |
| Fiscal Policies and Procedures | Permanent |
| Audits | Permanent |
| Financial statements | Permanent |
| General Ledger | Permanent |
| Check registers/books | 7 years |
| Business expenses documents | 7 years |
| Bank deposit slips | 7 years |
| Cancelled checks | 7 years |
| Investment records (deposits, earnings, withdrawals) | 7 years |
| Property/asset inventories | 7 years |
| Petty cash receipts/documents | 3 years |
| Credit card receipts | 3 years |

**Client Related Documentation**

The Company will retain the following documentation for at least six years from the date of its creation or the date when it last was in effect, whichever is later:

|  |  |
| --- | --- |
| Electronic Transaction Records |  |
| Client Profile Information |  |
| Information security and privacy policies and procedures implemented to comply with regulatory requirements |  |
| Third Party Agreements |  |

**Audit and Application Logs**

The Company will retain the following logs for at least one year from the date of its creation or the date when it last was in effect, whichever is later:

|  |  |
| --- | --- |
| Application logs (access, activity, error) |  |
| Infrastructure/Server/network Logs |  |
| Suspicious Transaction Alerts | Indefinitely |
| All intrusion detection logs |  |

**Data Disposal and Media Sanitization**

Any repurposed electronic media must be properly sanitized so that it does not contain any unauthorized accessible data. Appropriate techniques should be employed in the destruction of electronic media when methods to sanitize are unable to be applied.

**Repurposing Electronic Media**

Electronic Media must be *sanitized* before being repurposed. Data on devices that are no longer operational must be sanitized before the devices are reused. Sanitization must be done using procedures established by the Guidelines for Media Sanitization Recommendations from the [National Institute of Standards and Technology, NIST Special Publication 800-88.](https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final)

**Disposal & Destruction of Faulty Electronic Media**

Electronic Media must be *destroyed* when the device is faulty and contains operational Data. There are many different types, techniques, and procedures for media Destruction please see the above NIST document for details. The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

**Documentation**

Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. The certificate should record information about the media such as:

* Manufacturer/Model
* Serial Number
* Media Type (i.e., magnetic, flash memory, hybrid, etc.)
* Media Source (i.e., user or computer the media came from)
* Sanitization Description (i.e., Clear, Purge, Destroy)
* Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
* Tool Used (including version)
* Verification Method (i.e., full, quick sampling, etc.)
* Identification of person completing sanitization and verification, date and contact information
* Media Sanitization documentation should be retained indefinitely.

**Purpose**

The purpose of this Policy is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed by the company or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees in understanding their obligations in retaining electronic documents - including e-mail, messaging, Web files, text files, sound and movie files, PDF documents, client files and all other formatted files.

**Scope**

The scope of this policy and procedure is all data and removable media within <COMPANY NAME>’s systems.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 01.v - Information Access Restriction

Applicable Standards from the HIPAA Security Rule

* No Specific Standards

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |